

UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF CALIFORNIA

JOHN FINKELSTEIN, et al.,

Plaintiffs,

v.

SAN MATEO COUNTY DISTRICT
ATTORNEY'S OFFICE, et al.,

Defendants.

Case No. [18-cv-00009-EMC](#)

**ORDER GRANTING PLAINTIFFS'
MOTION FOR SUMMARY
ADJUDICATION; GRANTING
PLAINTIFFS' MOTION TO FILE A
SUR-REPLY; AND DENYING
COUNTY DEFENDANTS' MOTION
FOR SUMMARY JUDGMENT**

Docket Nos. 70, 81, 95

Plaintiffs John and Jennifer Finkelstein have filed a § 1983 civil rights action based on a search that the police conducted of their home and cars. Defendants are as follows:

- (1) Jeffrey S. Cichocki, a detective with the Loudoun County (Virginia) Sheriff's Office;
- (2) the City of San Mateo and Nicolas Ryan, a detective with the San Mateo Police Department ("SMPD") (collectively, the "City Defendants"); and
- (3) the San Mateo County District Attorney's Office and a deputy D.A. Vishal Jangla (collectively, the "County Defendants").

Plaintiffs have asserted the following claims for relief, all based on § 1983: (1) judicial deception (individual defendants only); (2) use of untrustworthy information to establish probable cause (individual defendants only); (3) use of untrustworthy information to procure a warrant (City and County only); (4) use of a search warrant application lacking probable cause on its face to procure a warrant (individual defendants only); (5) unreasonable search and seizure without a warrant, probable cause, and exigent circumstances (individual defendants only).

Currently pending before the Court are two motions: (1) Plaintiffs' motion for summary adjudication on the issue of probable cause and (2) the County Defendants' motion for summary

judgment. Having considered the parties' briefs and accompanying submissions, as well as the oral argument of counsel, the Court hereby **GRANTS** Plaintiffs' motion and **DENIES** the County Defendants' motion.

I. LEGAL STANDARD

Federal Rule of Civil Procedure 56 provides that a "court shall grant summary judgment [to a moving party] if the movant shows that there is no genuine dispute as to any material fact and the movant is entitled to judgment as a matter of law." Fed. R. Civ. P. 56(a). An issue of fact is genuine only if there is sufficient evidence for a reasonable jury to find for the nonmoving party. *See Anderson v. Liberty Lobby, Inc.*, 477 U.S. 242, 248-49 (1986). "The mere existence of a scintilla of evidence . . . will be insufficient; there must be evidence on which the jury could reasonably find for the [nonmoving party]." *Id.* at 252. At the summary judgment stage, evidence must be viewed in the light most favorable to the nonmoving party and all justifiable inferences are to be drawn in the nonmovant's favor. *See id.* at 255.

Where a plaintiff moves for summary judgment on claims that it has brought (*i.e.*, for which it has the burden of proof), it "must prove each element essential of the claims . . . by undisputed facts." *Cabo Distrib. Co. v. Brady*, 821 F. Supp. 601, 607 (N.D. Cal. 1992)

Similarly, where a defendant moves for summary judgment based on an affirmative defense (*i.e.*, an issue on which it bears the burden of proof), the defendant must establish "all of the essential elements of the . . . defense to warrant judgment in [its] favor." *Martin v. Alamo Cmty. College Dist.*, 353 F.3d 409, 412 (5th Cir. 2003) (internal quotation marks omitted; emphasis omitted); *see also Clark v. Capital Credit & Collection Servs.*, 460 F.3d 1162, 1177 (9th Cir. 2006) (noting that a defendant bears the burden of proof at summary judgment with respect to an affirmative defense).

Summary adjudication differs from summary judgment only in that a Court focuses on a limited issue as opposed to an entire claim or the entire action. *See Moxley v. Texaco, Inc.*, No. 00-1518 CM (BQRx), 2000 U.S. Dist. LEXIS 20255, at *7 (C.D. Cal. Dec. 19, 2000).

A. Relevant Factual Background

The Finkelsteins' home and cars were searched pursuant to a search warrant that was issued by the San Mateo County Superior Court. The state court approved the search warrant based on an affidavit submitted by Detective Ryan of the SMPD. The events that led to the warrant and search were as follows.

In November 2015, the Loudoun County (Virginia) Sheriff’s Office – where Detective Cichocki works – received a report of an unknown suspect “sexting” a female minor. *See* Alberts Decl., Ex. B (Cichocki Aff. at 3). The minor informed the police that “she had been contacted by ‘Peter Mayfair’ on an application called LOL” and that “[t]he conversation moved to Skype where she was encouraged by [him] bearing Skype Name ‘johrobbins6’ . . . to use the video function and show herself in various forms of undress.” Alberts Decl., Ex. B (Cichocki Aff. at 3). The minor showed her private areas to the suspect and eventually the suspect threatened her to “do exactly what I say and beg me or I will share this video on the internet.” Alberts Decl., Ex. B (Cichocki Aff. at 3). The suspect claimed that “he was using a proxy server and could not be traced.” Alberts Decl., Ex. B (Cichocki Aff. at 3).

Through an administrative subpoena served on Skype, the police learned that the screen name “johnrobbins6” “came back to an IP in Nam[i]bia, Africa,” which, according to the police, “substantiat[ed] the claim that [the suspect] was using a proxy server.” Alberts Decl., Ex. B (Cichocki Aff. at 3). The police also learned that the registered email that Skype had for “johnrobbins6” was johnrob@gmail.com.

“An administrative subpoena to [Google] returned with a user of John Robert Finkelstein.”

Alberts Decl., Ex. B (Cichocki Aff. at 4). The recovery email for johnrob@gmail.com was johnrob@cs.stanford.edu. *See* Alberts Decl., Ex. B (Cichocki Aff. at 4). Google also had a phone number listed for SMS, which the police then used to subpoena AT&T, and this led the police to Mr. Finkelstein in San Mateo. The email address for the AT&T account was also

1 johnrob@gmail.com.

2 Because Mr. Finkelstein was located in San Mateo, Detective Cichocki reached out to the
3 SMPD for assistance. In December 2015, Detective Ryan of the SMPD “was tasked with
4 assisting” Detective Cichocki in the investigation. *See* Merin Decl., Ex. A (Ryan Aff. at 4).
5 Detective Ryan ultimately prepared an affidavit to support the application for a search warrant on
6 the Finkelsteins’ home and cars. In his affidavit, Detective Ryan noted, *inter alia*, as follows:

- 7 • The victim was “contacted by an unknown subject on an application called MyLOL
8 where she was sent a message by a user with the profile name ‘Peter Mayfair.’ The
9 profile picture for this user was of a juvenile male with the stated birthday of
10 (01/03/1999).” Merin Decl., Ex. A (Ryan Aff. at 4). “MyLOL is a teenager social
11 networking/dating website.” Merin Decl., Ex. A (Ryan Aff. at 5).
- 12 • The suspect asked the victim to Skype him, and she eventually agreed. “The
13 suspect’s Skype profile name was ‘johnrobbins6.’” Merin Decl., Ex. A (Ryan Aff.
14 at 5). The profile also indicated that he was from London, England. *See* Merin
15 Decl., Ex. A (Ryan Aff. at 5).
- 16 • The suspect asked the victim for video via Skype, and “she used the video feature 2
17 or 3 times, but only spoke via text on Skype.” Merin Decl., Ex. A (Ryan Aff. at 5).
18 The suspect used the video feature but one time only, and the video simply
19 “showed a still image of a white juvenile male with brown hair.” Merin Decl., Ex.
20 A (Ryan Aff. at 5). The victim never saw the suspect, nor did she ever hear his
21 voice. *See* Merin Decl., Ex. A (Ryan Aff. at 5).
- 22 • The suspect asked the victim to show her breasts and genitalia via Skype video and
23 she did so. After she did so, the victim told the suspect she was leaving the chat
24 and the suspect threatened her, saying, *e.g.*, “‘I showed u a video that’s not even
25 me’ [and] ‘u will do exactly what I say and beg me or I will share this video on the
26 internet.’” Merin Decl., Ex. A (Ryan Aff. at 5). The suspect told the victim that
27 “he used a proxy server so he could not be traced, he had her phone number[] and
28 IP address, and he could find where she lived.” Merin Decl., Ex. A (Ryan Aff. at 5).

- Through an administrative subpoena on Skype, the police learned that the account for “johnrobbins6” was created in August 2015 from an IP address in Namibia, Africa, “which substantiated the suspect’s claim that he was likely using a proxy server.” Merin Decl., Ex. A (Ryan Aff. at 5). The police also learned that, “[i]n order to create a Skype account a valid email address is necessary. The email address used to create this account was johnrob@gmail.com.” Merin Decl., Ex. A (Ryan Aff. at 5).
- Through an administrative subpoena on Google, the police learned that “[t]he email account johnrob@gmail.com returned to a John Finkelstein and a recovery email address was listed as johnrob@cs.stanford.edu.” Merin Decl., Ex. A (Ryan Aff. at 5). Google also had a phone number listed for SMS. *See* Merin Decl., Ex. A (Ryan Aff. at 5).
- The police learned that the provider for the phone number was AT&T, and, through an administrative subpoena on AT&T, the police obtained the subscriber information for the phone number. AT&T identified the subscriber as John R. Finkelstein with an address in San Mateo. *See* Merin Decl., Ex. A (Ryan Aff. at 5).

In January 2016, a San Mateo superior court judge signed off on the search warrant application submitted by Detective Ryan. *See* Merin Decl., Ex. A (Ryan Aff. at 2). Subsequently, a search of the Finkelsteins’ home and cars (for child pornography) was conducted. It appears that, ultimately, nothing was found, and Mr. Finkelstein was never charged with any crime.¹

Thereafter, Mr. Finkelstein filed a motion in state court, challenging the search warrant and asking for a return of the property seized from him during the search. In October 2017, the superior court judge who signed off on the warrant issued an order on the motion favorable to Mr.

¹ At the hearing, Mr. Cichocki suggested, for the first time, that the state judge’s approval of the search warrant application precludes this Court from considering, in a § 1983 civil action, whether there was probable cause for the search based on the four corners of the application. Mr. Cichocki, however, provided no authority to support the position that a state court’s issuance of a warrant precludes a finding by a federal court that the warrant was constitutionally deficient. Interestingly, Mr. Cichocki does not argue that the subsequent ruling of the state court – *i.e.*, that the warrant was not legally obtained – is binding. *See* note 2, *infra*.

Finkelstein. The judge found, *inter alia*, that certain statements made in the Ryan affidavit in support of the search warrant were made in reckless disregard for the truth and, once these statements were excised, the remaining statements were insufficient to establish probable cause. *See* Merin Decl., Ex. E (Order at 4). The judge also found that, even if it were to interpret the misleading statements “in the manner consistent with the meaning the detectives” advocated, there was still no probable cause. Merin Decl., Ex. E (Order at 5). The affidavit “simply showed that Mr. Finkelstein’s email address was provided *along with other misinformation* when the Skype account was created. *Anyone could have randomly provided his email address during the creation of the Skype account.* Consequently, the affidavit failed to establish probable cause.”² Merin Decl., Ex. E (Order at 5) (emphasis added).

B. Probable Cause

In their motion for summary adjudication, Plaintiffs ask the Court to hold that (1) the police affidavit used to obtain the search warrant failed to establish probable cause and that (2) the search warrant was issued without probable cause.³

Under the Fourth Amendment, a search without probable cause is prohibited. “‘Probable cause for a search requires a fair probability that contraband or evidence of a crime will be found in a particular place, based on the totality of the circumstances.’” *United States v. Fries*, 781 F.3d 1137, 1150 (9th Cir. 2015). Fair probability does not mean “certainty or even a preponderance of the evidence,” *United States v. Gourde*, 440 F.3d 1065, 1069 (9th Cir. 2006), but “[m]ere suspicion, common rumor, or even strong reason to suspect are not enough.” *United States v. Lopez*, 482 F.3d 1067, 1072 (9th Cir. 2007).

Although probable cause is a legal question, “the factual matters underlying the judgment

² In their papers, Defendants suggest that, in assessing probable cause, the Court should give no consideration to the state court’s order discussed above. To the extent Defendants mean that the state court’s findings are not preclusive, they are correct but, that being said, Plaintiffs do not dispute such. Moreover, even if the Court were to effectively “strike” the state court’s order, that does not bar the Court from arriving at the same or similar conclusions on its own, based on the same or similar reasoning.

³ The Finkelsteins are moving for summary adjudication with respect to the issue of probable cause only. They are not asking the Court to make any ruling on judicial deception (as the state court did).

1 of reasonableness generally mean that probable cause is a question for the jury; and summary
2 judgment is appropriate only if no reasonable jury could find that the officers did or did not have
3 probable cause to [act].” *McKenzie v. Lamb*, 738 F.2d 1005, 1008 (9th Cir. 1984).

4 In the instant case, the Court finds that there are no genuine disputes of material fact
5 regarding probable cause. Moreover, because no reasonable juror could find probable cause based
6 on the undisputed facts, as discussed below, the Court grants Plaintiffs’ motion for summary
7 adjudication. The Court agrees with the analysis of the state court judge who signed off on the
8 warrant but then later found a lack of probable cause. At bottom, the sole link to Mr. Finkelstein
9 was the email given for the Skype account – johnrob@gmail.com – an email that could have been
10 given by anyone and that required no verification by Skype.

11 According to Defendants, there was probable cause for the search because there
12 circumstances tying Mr. Finkelstein to the crime in addition to the above email address. Those
13 other circumstances, however, are not meaningful. For example:

- 14 • The fact that the suspect’s public username on Skype was johnrobbins6 – *i.e.*, a
15 name consistent with the email address johnrob@gmail.com – shows nothing. The
16 suspect easily could have chosen the public username to be consistent with the
17 email address (or vice-versa) but that does not mean that the email address was the
18 suspect’s real email address (*i.e.*, that the Skype account belonged to the person
19 with the email address johnrob@gmail.com). In testimony before the state court,
20 D.D.A. Jangla asked, “if someone was simply trying to create a random Skype
21 account, why try to coordinate the user name – which in this case was johnrobbins6
22 – to the e-mail address used to open it – which was johnrob@gmail – as opposed to
23 just entering in random data”? Alberts Decl., Ex. E (Tr. at 74). But the easy
24 answer to this is convenience, especially where a person is trying to hide his
25 identity.
- 26 • The fact that the email address johnrob@gmail.com had, per Google, a recovery
27 email of johnrob@cs.stanford.edu shows nothing. That the second email address
28 was consistent with the first does not establish that the first email address was the

1 suspect's real email address (*i.e.*, that the Skype account belonged to the person
2 with the email address johnrob@gmail.com). The recovery email does nothing to
3 substantiate the weak link of the email address provided to Skype.

- 4 • Although Defendants argue that there was a fair probability that Mr. Finkelstein
5 was the perpetrator because the perpetrator was clearly tech savvy (*e.g.*, using a
6 proxy server to hide his identity) and Mr. Finkelstein is a software engineer from
7 Silicon Valley, that argument lacks merit because there is nothing in the Ryan
8 affidavit to indicate that either he, Detective Cichocki, or anyone else involved in
9 the investigation knew *at any time before the search* that Mr. Finkelstein is a
10 software engineer. Therefore, that fact cannot be a part of the probable cause
11 calculus. To the extent Defendants have tried to argue that the recovery email
12 address johnrob@cs.stanford.edu shows that Mr. Finkelstein worked for the
13 Computer Science Department at Stanford, *see* Docket No. 81 (County Mot. at 12),
14 that argument is unavailing because nothing indicates that Defendants knew that
15 the "cs" referred to the Computer Science Department. And even if Defendants
16 knew that, nothing shows that Defendants knew what Mr. Finkelstein did at the
17 Computer Science Department. Certainly no mention is made in the Ryan affidavit
18 submitted as part of the search warrant application.

19 At oral argument, Defendants alluded to the fact that they sought a search warrant only and
20 not a more intrusive arrest warrant. But, Defendants have not cited any authority to support the
21 proposition that the standard for probable cause for a search warrant materially differs from that
22 for an arrest warrant. In both situations, the question is whether there is a "fair probability." In
23 any event, in this case, if there was probable cause for a search warrant, there would have been
24 probable cause for an arrest warrant. The police wanted to search places within the possession,
25 custody, or control of Mr. Finkelstein (*i.e.*, his home and cars) for child pornography; if the police
26 had a fair probability that Mr. Finkelstein possessed that, the police would have had probable
27 cause to believe he committed the crime. *Cf. Chism v. Wash.*, 661 F.3d 380, 389 (9th Cir. 2011)
28 (noting that, in a prior case involving a search of a computer for child pornography, "we looked

for evidence in the affidavit: (1) that a crime was committed; (2) that it was Gourde who committed the crime; and (3) that evidence of the crime would be found in the place to be searched[;] [i]n light of this ‘triad of solid fact,’ we concluded that ‘the reasonable inference that Gourde had received or downloaded [child pornographic] images easily meets the “fair probability” test’”).

At the end of the day, the email address registered with Skype (johnrob@gmail.com) was the only link that Defendants had to tie Mr. Finkelstein with the crime. Anyone can establish a Skype account and list as a “valid” email someone else’s email address. Skype does not verify the email address given. *See, e.g.*, Docket No. 93-3 (Merin Decl., Ex. 2) (Tr. at 19-22) (Plaintiffs’ expert, Neil Broom, testifying in the state court proceedings that he was able to register and create a working Skype account using the email address barackobama@whitehouse.gov and that it is possible to use an email that does not actually exist to create a working Skype account). And there was nothing to corroborate that this email address supplied by the suspect was in fact the suspect’s real email address.

Moreover, there was actually evidence indicating that the suspect had supplied a false email address in registering with Skype. The suspect had taken multiple steps to conceal his identity – *e.g.*, using different names for his MyLOL and Skype accounts (Peter Mayfair and johnrobbins6, respectively), using a proxy server from Namibia,⁴ never showing his “live” face during the video exchange with the victim, never communicating orally with the victim, and using a picture of someone else during the video exchange (“I showed u a video that’s not even me”). As Plaintiffs argue, “[a]n email address provided by an internet criminal that has taken steps to conceal his identity [is] not reasonably trustworthy information that can support a finding of

⁴ *See* Alberts Decl., Ex. A (Tr. at 107) (Detective Cichocki testifying before the state court that, “through my training and experience with other cases and speaking with other law enforcement officials, that Namibia is a location that hosts proxy servers”); Alberts Decl., Ex. B (Officer Cichocki’s response to Rog No. 7 stating that he “spoke with several law enforcement officers to consult upon the fact that the suspect said he was using a proxy server and that the IP address via Nam[i]bia was most likely that”; adding that he “verified via the FBI that attempts to get further IP information via the Nam[i]bia connection would be fruitless”).

probable cause.”⁵ Reply to County at 3. *See generally United States v. Macias-Perez*, No. CR 11-2024, 2011 U.S. Dist. LEXIS 68305, at *40 (N.D. Iowa June 24, 2011) (stating that “the use of false names and identifying information is common in criminal society”). Whether Detective Ryan (or Detective Cichocki or anyone else) *could* have done more investigation – *e.g.*, per Plaintiffs, “to trace the [Namibian] IP address used by the suspect when the Skype account was created . . . or trace the IP address used by the suspect on November 24, 2015, the date that the ‘sexting’ incident is alleged to have occurred,” Mot. at 3, is not the question. The bottom line is that Defendants did not do more investigation, and the Court must assess probable cause based on what information Defendants did have when applying for the search warrant – which was simply an email address that had a great chance of being inaccurate (*i.e.*, not the suspect’s real email address).

The above analysis in and of itself is sufficient to establish a lack of probable cause for the search warrant. The analysis is consistent with the Ninth Circuit’s decision in *Chism*. The plaintiffs in *Chism* were a husband and wife, Todd and Nicole Chism. They filed a § 1983 suit after their home and Mr. Chism’s business office were searched for child pornography. The search did not reveal any evidence of child pornography and charges were never filed against Mr. Chism. The plaintiffs brought a claim for judicial deception and, in evaluating the claim and whether qualified immunity applied, the Ninth Circuit noted that, if false statements in the affidavit supporting the warrant application had been corrected, then the application would have reflected that Mr. Chism’s only connection to the pornographic websites at issue was a credit card. *See Chism*, 661 F.3d at 390 (stating that “[a] truthful version of [the officer’s] affidavit would have indicated that the sole evidence connecting Todd Chism [the plaintiff] to the child pornographic images was the fact that the credit card he shared with [his wife] Nicole was charged three times for hosting the websites that contained child pornographic images”). The court then

⁵ At the hearing, Defendants’ only real comeback was that it was not impossible that the perpetrator provided his real email address because criminals sometimes do stupid or foolish things (and thus get caught). Although the Court recognizes that criminals sometimes do stupid or foolish things, Defendants have provided no evidence – and there was nothing in the Ryan affidavit – to substantiate how often that is the case, or any reason to believe that is what occurred here.

indicated agreement with an expert that “relying only on information provided by the user of a credit card that is associated with criminal activity is *inherently unreliable*.” *Id.* at 391 (emphasis in original). The Court also approved a police training manual that stated

“[m]uch, if not all, of the cyber-evidence (the E-mail addresses and IP addresses used) will lead you to an innocent person,] [which is] why simply identifying which account was used to commit a crime does not provide you with probable cause . . . You’ll need to do more investigating to determine if there is a link between the account holder (or other members of the household) with the criminal activity that was committed with that account.”

Id.

A similar criticism is applicable in the instant case – *i.e.*, relying only on information provided by a person associated with criminal activity, particularly when the information provided is identifying information and the person has taken a fair amount of effort to conceal his identity, is inherently unreliable.

III. COUNTY DEENDANTS’ MOTION⁶

As noted above, the County Defendants are the County and D.D.A. Jangla. For the County Defendants’ motion, the parties have submitted evidence in addition to that provided for Plaintiffs’ motion. The additional evidence includes testimony from Plaintiffs’ expert, Neil Broom (provided during the state court proceedings); testimony from D.D.A. Jangla (also provided during the state court proceedings); and a declaration from Karen Guidotti, the Chief D.D.A. for the Country District Attorney’s Office.

The County Defendants argue that, based on the evidence submitted, they are entitled to summary judgment on each of the claims asserted against them.

A. First Cause of Action – Judicial Deception Claim

Plaintiffs’ first cause of action for judicial deception is asserted against the individual defendants only. The judicial deception claim against D.D.A. Jangla is premised on the fact that he allegedly approved the submission of the Ryan affidavit to the state court judge. D.D.A. Jangla argues that he has qualified immunity with respect to the judicial deception claim.

⁶ The Court grants Plaintiffs’ motion for leave to file a sur-reply as there is no apparent prejudice to the County Defendants. *See* Docket No. 95 (motion).

“Courts engage in a two-pronged analysis to determine whether qualified immunity applies: ‘[O]fficers are entitled to qualified immunity under § 1983 unless (1) they violated a federal statutory or constitutional right, and (2) the unlawfulness of their conduct was “clearly established at the time.”’” *Easley v. City of Riverside*, 890 F.3d 851, 856 (9th Cir. 2018).

In *Chism*, the Ninth Circuit held that “governmental employees are not entitled to qualified immunity on judicial deception claims.” *Chism*, 661 F.3d at 393. The reason why was fairly simple:

“[I]f an officer submitted an affidavit that contained statements he knew to be false or would have known were false had he not recklessly disregarded the truth and no accurate information sufficient to constitute probable cause attended the false statements, . . . he cannot be said to have acted in a reasonable manner, and the shield of qualified immunity is lost.”

Id.

Therefore, in order for a plaintiff “to survive a defendant officer’s motion for summary judgment on the ground of qualified immunity,” all that the plaintiff must do is “1) make a ‘substantial showing of deliberate falsehood or reckless disregard for the truth and 2) establish that, but for the dishonesty, the challenged action would not have occurred.” *Liston v. Cty. of Riverside*, 120 F.3d 965, 973 (9th Cir. 1997). The first element of a judicial deception claim – “a deliberate or reckless false statement or omission – is a question of fact,” even though “[t]he second element – materiality – is for the Court and may be decided on summary judgment.” *Rhabarian v. Cawley*, No. 2:10-cv-00767-TLN-KJN, 2013 U.S. Dist. LEXIS 112189, at *28-29 (E.D. Cal. Aug. 7, 2013); *see also Liston*, 120 F.3d at 974 (stating that, “[w]hile the materiality issue is one ‘reserved to the court,’ if the [plaintiffs] make the required ‘substantial showing,’ the question of intent or recklessness is ‘a factual determination for the trier of fact’”).

In the instant case, given that the evidence must be viewed in the light most favorable to the Finkelsteins, *see id.* at 974-75, they have made out a substantial showing on the first element above, *i.e.*, that a deliberate or reckless false statement or omission was made. A reasonable jury could find, just as the state court did, that, when Detective Ryan stated the following in his affidavit – “In order to create a Skype account a valid email address is necessary. The email

1 address *used to create this account* was johnrob@gmail.com,” Merin Decl., Ex. A (Ryan Aff. At
2 6) (emphasis added) – he made a false statement. The state court found that “the meaning
3 intended by the phrase ‘used to create this account’ was that the owner of the email account ‘used’
4 the email account in a manner *involving control* over the email account by the owner.” Merin
5 Decl., Ex. E (Order at 4) (emphasis added). The state court added that this statement was made in
6 reckless disregard for the truth “because the email address was not ‘used’ but instead was simply
7 included along with other requested information by the individual who created the Skype account
8 and had no reason to supply any accurate information.” Merin Decl., Ex. E at 4). Thus, the police
9 affidavit implied that there was a real connection between the Skype account and Mr. Finkelstein
10 when in fact the factual basis for that implication was lacking. The misleading nature of the
11 affidavit was amplified by the fact that Detective Ryan failed to clarify that a “valid” email is not a
12 verified email.

13 While the above analysis applies to Detective Ryan, and the moving party here is D.D.A.
14 Jangla, D.D.A. Jangla allegedly reviewed and approved the search warrant application submitted
15 by Detective Ryan. Thus, it is plausible that D.D.A. Jangla had as much knowledge as Detective
16 Ryan as to the misleading nature of the affidavit.

17 To be clear, the Court is not making any ruling at this juncture that there was, in fact,
18 judicial deception on the part of D.D.A. Jangla. Indeed, a reasonable jury might well find
19 otherwise. But given that all reasonable inferences must be drawn in Plaintiffs’ favor, summary
20 judgment must be denied.

21 B. Second and Fourth Causes of Action – Use of Untrustworthy Information to Establish
22 Probable Cause and Use of Search Warrant Application Lacking Probable Cause on Its
23 Face

24 As with the first cause of action above, Plaintiffs’ second and fourth causes of action –
25 both related to a lack of probable cause – are asserted against the individual defendants only.
26 D.D.A. Jangla argues that he has qualified immunity with respect to these claims as well, which
27 seem to be predicated on his approval of the Ryan affidavit for submission to the state court.

28 As an initial matter, the Court takes note that D.D.A. Jangla argues for a broad application

of qualified immunity based on the second prong of the doctrine – *i.e.*, liability is dependent on there being *clearly established* unlawful conduct. D.D.A. Jangla points out that, in *White v. Pauly*, 137 S. Ct. 548 (2017), the Supreme Court stated that it is a “longstanding principle that ‘clearly established law’ should *not* be defined ‘at a high level of generality’” because, “[o]therwise, ‘[p]laintiffs would be able to convert the rule of qualified immunity . . . into a rule of virtually unqualified liability simply by alleging violation of extremely abstract rights.” *Id.* at 552 (emphasis added). The Supreme Court criticized the lower appellate court’s decision because

[i]t failed to *identify a case* where an officer acting under similar circumstances as Officer White was held to have violated the Fourth Amendment. Instead, the [panel] majority relied on *Graham*, *Garner*, and their Court of Appeals progeny [excessive force cases], which . . . lay out excessive-force principles at only a general level. Of course, “general statements of the law are not inherently incapable of giving fair and clear warning to officers, but “in the light of pre-existing law the unlawfulness must be apparent.” For that reason, we have held that *Garner* and *Graham* do not themselves create clearly established law outside “an obvious case.”

Id. (emphasis added). The Supreme Court added that “[t]his is not a case where it is obvious that there was a violation of clearly established law under *Garner* and *Graham*”; the case was not a run-of-the mill Fourth Amendment violation but rather presented unique facts and circumstances. *Id.*

D.D.A. Jangla overstates the reach of *White*. He suggests that *White* “stands for the proposition that in order to demonstrate that the law was ‘clearly established,’ a plaintiff must identify a published opinion addressing nearly identical facts that concludes that an officer violated the Constitution.” *McKenney v. Mangino*, No. 2:15-cv-00073-JDL, 2017 U.S. Dist. LEXIS 55649, at *22 (D. Me. Apr. 12, 2017). But, in *McKenney*, the Supreme Court only “faulted the lower court for failing to identify a case with similar factual circumstances” because the case presented a unique set of facts and circumstances. *Id.* at *23-24. “Because Officer White’s conduct [in *White*] did not amount to a ‘run-of-the-mill constitutional violation, a case with similar facts would be required to put the officer on notice that his conduct violated clearly established law.” *Id.* at *24. “As a practical matter, the standard advanced by [the defendant officer] fails to account for the reality that the factual circumstances of each case are, by their

1 nature, unique, and two cases seldom involve nearly identical facts. Courts should therefore look
2 to cases that analyze similar circumstances.” *Id.* at 25. “A case presenting a nearly identical
3 alignment of facts is not required so long as the existing cases would enable an officer, as a matter
4 of reason and common sense, to understand that his or her conduct in a specific situation crossed
5 the constitutional line.” *Id.*

6 Plaintiffs argue that *Chism*, 661 F.3d at 380, fits this criteria. While there is language in
7 *Chism* that strongly supports Plaintiffs’ position, *Chism* arguably is not dispositive because the
8 Ninth Circuit’s holding was not predicated solely on the false statements made in the police
9 affidavit. The Ninth Circuit did not hold that the false statements when corrected (*i.e.*, to show
10 that the only connection between Mr. Chism and the websites was the credit card) alone
11 established a lack of probable cause. Rather, the Ninth Circuit’s ruling took into account both the
12 correction of false statements and the supplementation of information that had been omitted (*i.e.*,
13 IP addresses traced to persons other than the Chisms).

14 But even assuming *Chism* is not dispositive, the facts in the instant case – *i.e.*, that
15 identifying information (such as an email address) provided by a person intent on hiding his
16 identity is likely unreliable – presents an obvious situation where probable cause is lacking. Thus,
17 *White* would not afford qualified immunity on the probable cause question. *See also Easley v.*
18 *City of Riverside*, 890 F.3d 851, 855-56 (9th Cir. 2018) (noting that “[t]he doctrine [of qualified
19 immunity] is designed to balance “two important, competing interests: the need to hold public
20 officials accountable for irresponsible actions, and the need to shield them from liability when
21 they make *reasonable* mistakes”) (emphasis added).

22 D.D.A. Jangla argues he is nonetheless entitled to qualified immunity because he “was in a
23 different position than Detectives Ryan or Cichocki. His only involvement with the search
24 warrant was that Detective Ryan asked him to determine whether Detective Ryan’s affidavit
25 should be submitted to a judge for a determination of probable cause.” Mot. at 10-11. But all
26 reasonable inferences must be drawn in favor of the party opposing summary judgment, and, for
27 purposes of this motion, the Court must infer that D.D.A. Jangla did not have a reasonable belief
28 that there was probable cause to support the warrant application. *See id.* at 856 (noting that, as

part of the qualified immunity analysis, a court must ask “whether the facts as alleged could support a reasonable belief that the conduct in question conformed to the established law”). This is a question that cannot be resolved on a motion to dismiss.⁷

C. Fifth Cause of Action – Unreasonable Search and Seizure Without a Warrant, Probable Cause, and Exigent Circumstances

The fifth cause of action is essentially a claim for unreasonable search and seizure based on a lack of probable cause. It is asserted against the individual defendants only and is predicated not on the initial seizure but on the fact that Detective Ryan and D.D.A. Jangla “turned over to [Detective] CICHOCKI computers, hard drives and cell phones seized . . . so that they could be searched in Virginia” and “[Detective] Cichocki then had this seized property unlawfully searched and forensically examined in Virginia without a warrant, judicial authorization, probable cause or exigent circumstances.” Compl. ¶ 124. As to this cause of action, D.D.A. Jangla makes two arguments: (1) there was no violation of the Finkelsteins’ constitutional rights because “[t]here is no case law in this Circuit holding that a person has a Constitutional right for his or her seized property to remain in the jurisdiction where the search warrant was issued,” Mot. at 13, and (2) even if the Finkelsteins “had a Constitutional right for their seized electronics to remain in California, such right was not ‘clearly established’ in the spring of 2016.” Mot. at 14.

To the extent the Finkelsteins are claiming a constitutional right not to have their property turned over to a different law enforcement agency, D.D.A. Jangla has a strong argument that there is no such constitutional right or, at the very least, he is protected by qualified immunity because such a right was not clearly established. While the Finkelsteins argue that the “transfer [of the property] was prohibited by Cal. Pen. Code §§ 1528(a) and 1536,” Opp’n at 18, that is not a constitutional right but rather a state statutory right.

However, it appears that the fifth cause of action is not necessarily about the *transfer* per se; rather, it also seems to encompass the fact that, once property (*i.e.*, computers, hard drives, and

⁷ Notably, D.D.A. Jangla asserts only qualified immunity, not prosecutorial immunity in his act of reviewing the proposed search warrant. *Cf. Patterson v. Yamhill Cty.*, No. 3:14-cv-00501-BR, 2015 U.S. Dist. LEXIS 131036, at *10 (D. Or. Sep. 29, 2015) (“Defendant is absolutely immune from suit for the prosecutorial act of *presenting* the arrest warrant to Judge Tichenor.”).

cell phones) was seized, it was *then* searched. According to the Finkelsteins, that search should not have taken place because there was no probable cause. The County Defendants have not explained why this theory is not viable. Accordingly, the County Defendants’ motion is denied to the extent Plaintiffs’ theory is an improper search (rather than an improper transfer).

D. Third Cause of Action – Use of Untrustworthy Information to Procure a Warrant

Unlike the other causes of action above, the third cause of action has been asserted against the entity defendants only, *i.e.*, the County and City. In the pending motion, the County Defendants argue that the County is entitled to summary judgment on the third cause of action because there is insufficient evidence to support *Monell* liability. *See Monell v. Dep’t of Soc. Servs.*, 436 U.S. 658 (1978).

It is well established that a municipality may be held liable for a violation of 42 U.S.C. § 1983. But “Congress did not intend to create *respondeat superior* liability”; rather, it

intended to hold municipalities liable only when action pursuant to official municipal policy of some nature caused a constitutional tort. The official policy requirement was intended to distinguish acts of the *municipality* from acts of *employees* of the municipality, and thereby make clear that municipal liability is limited to action for which the municipality is actually responsible.

Although a constitutional violation must result from official municipal policy, a county need not expressly adopt the policy. It is sufficient that the constitutional violation occurred pursuant to a longstanding practice or custom.

Christie v. Iopa, 176 F.3d 1231, 1235 (9th Cir. 1999) (emphasis in original; internal quotation marks omitted). In certain situations, deliberate indifference to a risk of constitutional violations can also be deemed a policy or custom. *See Flores v. Cty. of L.A.*, 758 F.3d 1154, 1157 n.8 (9th Cir. 2014) (noting that, “[u]nder *City of Canton v. Harris*, ‘[o]nly where a municipality’s failure to train its employees in a relevant respect evidences a deliberate indifference to the rights of its inhabitants can such a shortcoming be properly thought of as a city policy or custom under § 1983’[;] [w]here deliberate indifference is proved, ‘failure to provide proper training may fairly be said to represent a policy for which the city is responsible, and for which the city may be held liable if it actually causes injury’”).

In the instant case, the County argues that there is no evidence to support municipal

liability because, *e.g.*, the Finkelsteins cannot establish a failure to train that amounted to deliberate indifference. *See, e.g.*, Guidotti Decl. ¶ 6 (testifying that the County District Attorney’s Office “provides onsite training on Penal Code section 1524, the legal standards for motions to quash and traverse search warrants, and the components of a search warrant application”); *see also* Jangla Decl. ¶ 3 (testifying about training facilitated by County District Attorney’s Office). The County also notes that there is no indication that a final policymaker ratified D.D.A. Jangla’s actions vis-à-vis the search warrant application, and hence there is no *Monell* liability under a ratification theory. *See Christie*, 176 F.3d at 1238 (noting that a municipality “can be liable for an isolated constitutional violation if the final policymaker ‘ratified’ a subordinate’s actions”).

In response, the Finkelsteins argue that D.D.A. Jangla provided testimony before the state court that “is sufficient to create a question of material fact.” Opp’n at 19. D.D.A. Jangla’s testimony was as follows:

- A. Look I think the question is, you know, you could task an investigator with doing an infinite amount of investigative steps before submitting an investigation.
- The question is what is a reasonable investigative technique to try to get a suspect and to have sufficient probable cause? That’s the question. What is the standard practice and what is an acceptable practice as opposed to what is ideal in theory.
- And so, what I can tell you about is what is a standard practice and acceptable practice. And as I indicated, I have reviewed a lot of these electronic warrants. And I have not come across an investigation, in the warrants I have reviewed or in the trainings that I have attended, where a step has been to verify that the service [such as Skype] validates the e-mail address [*i.e.*, sends a confirming email to the email address submitted by the user].
- Q. Do you think it is reasonable to rely on the documents that you get from a corporation, in this case, Skype?
- A. That’s what we have to go on. So, yes, of course.
- Q. And would that be the standard practice, in your opinion, for detectives or officers writing search warrants?
- A. Always.

Merin Decl., Ex. 1 (Tr. at 29-30).

1 Viewing the above testimony, including all reasonable inferences drawn therefrom, in
2 Plaintiffs' favor, the Court agrees that there is a question of fact that precludes summary judgment
3 in the County's favor. D.D.A. Jangla's testimony suggests that it was the practice of the County to
4 accept an email address given to a provider such as Skype at face value – *i.e.*, not to investigate an
5 email address further to determine whether the email address provided did in fact belong to the
6 person who provided it.


7 **IV. CONCLUSION**

8 For the foregoing reasons, Plaintiffs' motion for summary adjudication is granted and the
9 County Defendants' motion for summary judgment is denied.

10 This order disposes of Docket Nos. 70, 81, and 95.

11
12 **IT IS SO ORDERED.**

13
14 Dated: November 21, 2018

15
16 
17 EDWARD M. CHEN
18 United States District Judge
19
20
21
22
23
24
25
26
27
28